

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-285283

(43)Date of publication of application : 12.10.2001

(51)Int.Cl. H04L 9/32
 G09C 1/00
 H04L 9/08
 H04L 12/28
 H04L 12/66

(21)Application number : 2000-094840

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 30.03.2000

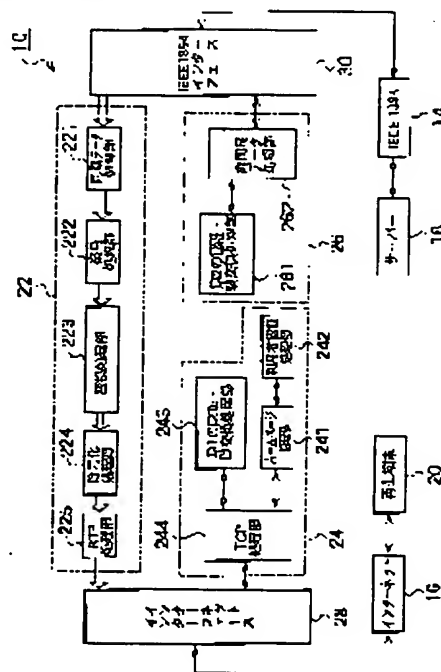
(72)Inventor : SAITO TAKESHI

(54) COMMUNICATION UNIT AND ITS COMMUNICATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a communication unit that can realize protection of copyright in the case of transmitting data from a home network to a public network and to provide its communication method.

SOLUTION: The communication unit interconnects a public network 16 such as the Internet and a home network 14 such as a network in compliance with the IEEE 1394. This communication unit consists of a 1st authentication/key exchange processing section 243 that performs authentication/key exchange with a reproduction terminal 20 connected to the public network 16, a 2nd authentication/key exchange processing section 261 that performs authentication/key exchange with a server 18 connected to the home network 14, a transmission section 22 that transmits AV data that are encrypted for copyright protection and obtained from the server 18 to the reproduction terminal 20, and a user authentication processing section 242 that authenticates a user of the reproduction terminal 20 and rejects communication with the reproduction terminal 20 when the user cannot be authenticated.



LEGAL STATUS

[Date of request for examination] 20.09.2001

[Date of sending the examiner's decision of rejection] 11.01.2005

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection] 2005-002443

[Date of requesting appeal against examiner's decision of rejection] 10.02.2005

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-285283

(P2001-285283A)

(43) 公開日 平成13年10月12日 (2001. 10. 12)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード (参考)
H 0 4 L 9/32		G 0 9 C 1/00	6 6 0 E 5 J 1 0 4
G 0 9 C 1/00	6 6 0	H 0 4 L 9/00	6 7 3 A 5 K 0 3 0
H 0 4 L 9/08			6 0 1 D 5 K 0 3 3
12/28		11/00	3 1 0 A 9 A 0 0 1
12/66		11/20	B

審査請求 未請求 請求項の数13 O L (全 9 頁)

(21) 出願番号 特願2000-94840 (P2000-94840)

(22) 出願日 平成12年3月30日 (2000. 3. 30)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 斉藤 健

神奈川県川崎市幸区小向東芝町1 株式会
社東芝研究開発センター内

(74) 代理人 100083806

弁理士 三好 秀和 (外7名)

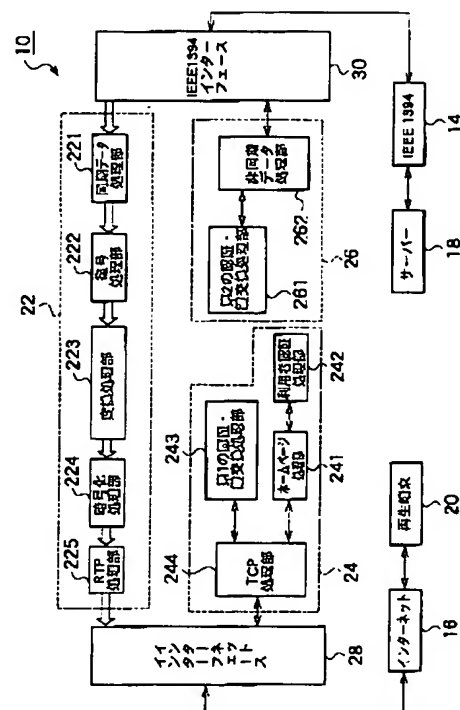
最終頁に続く

(54) 【発明の名称】 通信装置およびその通信方法

(57) 【要約】

【課題】 家庭網から公衆網へデータを送信する際の著作権保護を実現する通信装置およびその通信方法を提供する。

【解決手段】 インターネット等の公衆網16とIEEE1394等の家庭網14を結ぶ通信装置である。この通信装置は、公衆網16に接続された再生端末20との間で、認証・鍵交換を実行する第1の認証・鍵交換処理部243と、家庭網14に接続されたサーバー18との間で、認証・鍵交換を実行する第2の認証・鍵交換処理部261と、サーバー18から得られた、著作権保護のために暗号化されたAVデータを、再生端末20に送信する送信部22と、再生端末20の利用者を認証し、その利用者の認証ができない場合には、再生端末20との通信を拒絶する利用者認証処理部242と、から構成される。



1

【特許請求の範囲】

【請求項1】 公衆網である第1の網とローカルエリアネットワークである第2の網の間に配置され、該第1の網に接続された第1の端末と該第2の網に接続された第2の端末の間で暗号化データを転送する通信装置であって、

前記第1の端末との間で、認証・鍵交換を実行する第1の認証・鍵交換部と、

前記第2の端末との間で、認証・鍵交換を実行する第2の認証・鍵交換部と、

前記第2の端末から得られた暗号化データに、所定の変換を施し、かつ該データにあらかじめ付加されていた暗号制御情報と同一あるいは類似した暗号制御情報を付加して、前記第1の端末に送信する送信部と、

前記第1の端末の利用者を認証し、該利用者の認証ができない場合には、前記第1の端末との通信を拒絶する利用者認証部とを有することを特徴とする通信装置。

【請求項2】 前記第1の認証・鍵交換部は、前記第1の端末からの、前記第2の端末に対するデータ送信要求を、前記第2の端末に通知する手段を備える、ことを特徴とする請求項1に記載の通信装置。

【請求項3】 前記送信部は、前記第2の端末から得られた暗号化データを復号する手段、該復号されたデータに対して前記所定の変換を施す手段、および、該変換されたデータを暗号化する手段、を備える、ことを特徴とする請求項1に記載の通信装置。

【請求項4】 前記変換手段は、データ圧縮符号化方式およびデータ圧縮符号化速度のうちの少なくとも一方を変換する、ことを特徴とする請求項3に記載の通信装置。

【請求項5】 前記利用者認証部は、正規の利用者の識別IDおよび該識別IDに対応するパスワードをあらかじめ登録する利用者情報登録手段を備える、ことを特徴とする請求項1に記載の通信装置。

【請求項6】 前記第2の端末に通知する手段は、前記第1の端末の利用者の認証ができた場合のみ、前記第1の端末からのデータ送信要求を受け付ける、ことを特徴とする請求項2に記載の通信装置。

【請求項7】 前記第1の認証・鍵交換部は、前記第1の端末の利用者の認証ができた場合のみ、前記第1の端末との間の認証・鍵交換を実行する、ことを特徴とする請求項1に記載の通信装置。

【請求項8】 公衆網である第1の網に接続された第1の端末とローカルエリアネットワークである第2の網に接続された第2の端末との間で暗号化データを転送する通信方法であって、

前記第1の端末の利用者を認証する工程と、
該利用者の認証ができた場合のみ、前記第2の端末から暗号化データを取得する工程と、

該取得された暗号化データに、所定の変換を施し、かつ

2

該データにあらかじめ付加されていた暗号制御情報と同一あるいは類似した暗号制御情報を付加して、前記第1の端末に送信する工程とを含むことを特徴とする通信方法。

【請求項9】 前記利用者を認証する工程は、前記利用者から識別IDおよび該識別IDに対応するパスワードを取得するステップ、および、該取得された識別IDおよびパスワードが、あらかじめ登録された、正規の利用者の識別IDおよび該識別IDに対応するパスワードと、一致するか否かを照合するステップ、を含むことを特徴とする請求項8に記載の通信方法。

【請求項10】 前記第1の端末に送信する工程は、前記第2の端末から得られた暗号化データを復号するステップ、該復号されたデータに対して前記所定の変換を施すステップ、および、該変換されたデータを暗号化するステップ、を含むことを特徴とする請求項8に記載の通信方法。

【請求項11】 前記第2の端末から暗号化データを取得する工程の前後いずれかに、前記第2の端末との間で、認証・鍵交換を実行する工程、をさらに含む、ことを特徴とする請求項8に記載の通信方法。

【請求項12】 前記第1の端末に送信する工程の前後いずれかに、前記第1の端末との間で、認証・鍵交換を実行する工程、をさらに含む、ことを特徴とする請求項8に記載の通信方法。

【請求項13】 前記第1の端末に送信する工程の前後いずれかに、前記第1の端末からの認証・鍵交換要求を受け取る工程、および、前記第1の端末の利用者の認証ができた場合のみ、前記第1の端末との間で、認証・鍵交換を実行する工程、をさらに含む、ことを特徴とする請求項8に記載の通信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、IEEE1394等の家庭網とインターネット等の公衆網を結合する通信装置に係り、特に、著作権保護を考慮して家庭網から公衆網にデータを送信する通信装置、およびその通信方法に関する。

【0002】

【従来の技術】近年、情報のデジタル技術の進化に伴い、インターネットやホームネットワーク等が急速に普及して来ている。これにより、インターネット接続機能を持った家電機器や、家庭網とインターネットを接続する新しいゲートウェイ等、新しい市場が開けつつある。

【0003】たとえば、IEEE1394等の家庭網（ホームネットワーク）とインターネット等の公衆網とを結び付けるホームゲートウェイに関しては、ストレージ（蓄積）機能を持たせたり、デジタル放送受信機能を持たせる等、多くのアイデアが存在する。その中でも特に、ホームネットワークからのオーディオ・ビジュアル・デー

3

タ(AVデータ)を受信し、その受信されたAVデータを、たとえばエムペグー4(MPEG-4)等に圧縮した後、インターネット側に送信する、という注目すべきアイデアがある。これは、外出先から、家庭内のAVコンテンツを閲覧可能にしたり、家庭内の監視カメラによって撮影されたAVデータを、家庭外から参照可能にする等、多くのアプリケーションが考えられるからである。

【0004】

【発明が解決しようとする課題】ホームネットワーク上を流れるAVデータには、映画や音楽、音声、テレビ番組等、の著作物が含まれている場合がある。もちろん、AVデータ自身が著作物である場合もある。このような著作物を含む、あるいは著作物自体であるAVデータは、著作権による保護のため、ホームネットワーク上では暗号化されて送信される場合が多い。このため、ホームネットワーク上で入手された、暗号化AVデータをインターネットに再送信する場合、暗号化AVデータを一旦復号し、その暗号化を解除する必要がある。しかし、その復号されたAVデータをそのまま暗号化せずに、インターネット側に送信したのでは、今度は、インターネット上における著作権保護の意味が失われてしまうことになる。

【0005】一方、ホームゲートウェイが置かれている家庭の利用者以外からの、家庭内のAVコンテンツの閲覧・参照等の要求に対して、不用意に答えてしまうと、インターネットを介して不特定多数にコンテンツを送信してしまうことになりかねない。このことは、著作権法上で定められた「個人で楽しむ限りにおいては、タイムシフトや加工等が許される」という原則に反することになる。

【0006】このように、従来においては、ホームネットワークからインターネットに供給される著作物の送信については、著作権保護の観点からは、未だ不十分である。

【0007】本発明は、このような課題を解決し、家庭網から公衆網へデータを送信する際の著作権保護を実現する通信装置およびその通信方法を提供することを目的とする。

【0008】

【課題を解決するための手段】上記課題を解決するため、本発明は、第1の網(公衆網)16と第2の網(家庭網、ローカルエリアネットワーク)14の間に配置され、公衆網16に接続された第1の端末(再生端末)20と家庭網14に接続された第2の端末(サーバー)18の間で暗号化データを転送する通信装置であることを特徴とする。

【0009】より詳細には、本発明の第1の特徴は、上記の通信装置であって、再生端末20との間で、認証・鍵交換を実行する第1の認証・鍵交換部243と、サーバー18との間で、認証・鍵交換を実行する第2の認証・鍵交換部261と、サーバー18から得られた暗号化

4

データに、所定の変換を施し、かつその暗号化データにあらかじめ付加されていた暗号制御情報と同一あるいは類似した暗号制御情報を付加して、再生端末20に送信する送信部22と、再生端末20の利用者を認証し、その利用者の認証ができない場合には、再生端末20との通信を拒絶する利用者認証部242と、から構成される通信装置であることを第1の特徴とする。ここで、「暗号化データ」とは、少なくとも一部に著作物を含む、テキストや、写真、イラスト、絵画、アニメ、映画、音楽、音声、テレビ番組、WWWデータ等であって、著作権法による保護のために暗号化されているものである。

「所定の変換」とは、データ圧縮符号化方式およびデータ圧縮符号化速度のうちの少なくとも一方を変換することを意味する。より具体的には、家庭網14上を流れる暗号化データのデータ圧縮符号化方式、符号化速度を、公衆網16に適した符号化方式、符号化速度に、変換することである。「暗号制御情報」とは、サーバー18から得られたデータの録画やコピーを制御する情報である。たとえば、これ以上コピーを認めないという“No More Copy”である。

【0010】本発明の第1の特徴によれば、再生端末20の利用者を認証することで、サーバー18内のデータを要求する利用者が、正規の人物であることを十分に予想することができる。このため、利用者の認証以降の手順が、その利用者が個人的に楽しむための手順であることが明らかとなる。したがって、このことから、著作権法上で定められた「個人で楽しむ限りにおいては、タイムシフトや加工等が許される」という原則を遵守することが可能となる。

【0011】さらに、あらかじめ付加されていた、“No More Copy”等の暗号制御情報を、再生端末20に送信する際にも付加するので、元々のコピー制御の指定を守ることができる。このため、たとえば、録画やコピーをしてはいけない、と指定されていたデータは、再生端末20に送信する際も、録画やコピーを未然に防止する形式にすることができる。

【0012】本発明の第2の特徴は、上記の第1の特徴で述べた通信装置が実現する通信方法に係る。すなわち、第1の網(公衆網)16に接続された第1の端末(再生端末)20と第2の網(家庭網、ローカルエリアネットワーク)14に接続された第2の端末(サーバー)18との間で暗号化データを転送する通信方法であり、再生端末20の利用者を認証する工程と、その利用者の認証ができた場合のみ、サーバー18から暗号化データを取得する工程と、その取得された暗号化データに、所定の変換を施し、かつその暗号化データにあらかじめ付加されていた暗号制御情報と同一あるいは類似した暗号制御情報を付加して、再生端末20に送信する工程と、を少なくとも含む通信方法であることである。

【0013】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態について詳細に説明する。以下の図面の記載において、同一または類似の部分には同一または類似の符号を付している。

【0014】図1は、本発明の実施の形態に係る通信装置が配置された、ネットワーク・システムの全体構成を示すブロック図である。図1に示すように、本発明の実施の形態に係る通信装置10は、家庭12内に配設され、IEEE1394等で構成された家庭網14と、家庭12外に配設され、インターネット等で構成された公衆網16と、の間に接続される。家庭網14には、様々なAVデータを格納するサーバー18が接続され、このサーバー18内に蓄積されたAVデータは、通信装置10によって、家庭網14から公衆網16に送信される。公衆網16には、AVデータを再生することができる再生端末20が接続され、この再生端末20は、公衆網16を介して、通信装置10から送信されたAVデータを受信する。そして、再生端末20は、その受信されたAVデータを、再生する。

【0015】AVデータとしてはたとえば、テキストや、写真、イラスト、絵画、アニメ、映画、音楽、音声、テレビ番組、WWWデータ等が挙げられる。ここでは、説明の簡単化を図るため、AVデータの一部に著作物が含まれる、あるいはAVデータ自体が著作物であるとする。また、再生端末20は、AVデータの種類によって、種々の形態を採りうるものであり、たとえばAVデータが映像であれば、再生端末20はビューアとなる。もちろん、再生端末20は、据え置き型のものであっても、持ち運びを前提にした携帯端末のいずれであっても構わない。

【0016】図1では、家庭網14および公衆網16からなるネットワークには、3つの通信ノード、すなわち通信装置10、サーバー18および再生端末20が接続されているが、これ以外の通信ノードが接続されていても、もちろん構わない。

【0017】本発明の実施の形態に係る通信装置10は、異種のネットワークである、家庭網14と公衆網16とを結合する、ホームゲートウェイの役目を担うものである。この通信装置10の接続によって、異なる通信プロトコルを使っている家庭網14と公衆網16との間で、データのやりとりが可能となる。通信装置10はたとえば、家庭網14から公衆網16へデータを送信する場合には、その送信されるデータを公衆網16が使用するプロトコルと互換性のある形式に変換する。

【0018】また、本発明の実施の形態に係る通信装置10は、公衆網16側から家庭網14に接続された、サーバー18や、デジタルAV機器（たとえばDVDプレーヤ、据置型VTR、カメラ型VTR等）（図示しない）、の制御を可能とする機能を備える。

【0019】さらに、本発明の実施の形態に係る通信装置10は、サーバー18やデジタル機器から出力された

AVコンテンツを、リアルタイムにMPEG-4等の高圧縮のAVデータに変換し、その変換されたAVデータを公衆網16側に送信する機能を備える。ここで、このような変換機能が備えられるのは、通常、家庭12内に配設される家庭網14と比べて、インターネット等の公衆網16の通信帯域が非常に細く、このため、家庭網14上のAVデータをそのまま公衆網16に流すことはできないからである。したがって、たとえばIEEE1394からなる家庭網14上でやりとりされるMPEG-2データは、MPEG-4データに変換された後に、公衆網16に送信されることになる。

【0020】さて、図1に示したネットワーク・システムでは、著作権保護のため、家庭網14上でやりとりされるAVデータを暗号化処理する場合がある。本発明の実施の形態に係る通信装置10は、暗号化処理されたAVデータについても、そのAVデータを家庭網14から公衆網16に送信する場合には、上記のようなMPEG-2符号からMPEG-4符号への変換を実行する。ここで、この符号変換の際には、暗号化されたAVデータは一旦復号される。そして、変換終了後、変換後のAVデータは、再び暗号化されて、公衆網16側に送信されることになる。さらに、この実施の形態に係る通信装置10は、AVデータの暗号化処理のため、上記の変換処理および暗号化・復号処理に先立って、家庭網14側および公衆網16側の両方との間で、認証・鍵交換処理を実行する。

【0021】次に、図1および図2を用いて、本発明の実施の形態に係る通信装置10の構成について説明する。図2は、本発明の実施の形態に係る通信装置10の構成を示すブロック図である。図2では、説明の簡単化を図るため、図1の家庭網14としてIEEE1394バスを、公衆網16としてインターネットを採用した場合を示す。さらに、IEEE1394バス14からインターネット16へのデータ送信の際、そのデータはMPEG-2符号からMPEG-4符号に変換されるものとする。

【0022】図2に示すように、本発明の実施の形態に係る通信装置10は、IEEE1394バス14からインターネット16に送信されるAVデータの符号変換および暗号化・復号を実行する送信部22と、インターネット16側との認証・鍵交換処理を実行する第1の認証・鍵交換部24と、IEEE1394バス14側との認証・鍵交換処理を実行する第2の認証・鍵交換部26と、送信部22および第1の認証・鍵交換部24とインターネット16との間を結ぶインターネットインターフェース28と、送信部22および第2の認証・鍵交換部26とIEEE1394バス14との間を結ぶIEEE1394インターフェース30と、を備える。

【0023】ここで、送信部22は、IEEE1394インターフェース（以下、単に「IEEE1394I/F」と呼ぶ）30と接続し、IEEE1394バス14からのAVデータを受信する同期データ処理部221と、同期データ処理部221と接続し、受信されたAVデータを復号する復号処理部222

7

と、復号処理部222と接続し、復号されたAVデータ（MPEG-2データ）をMPEG-2符号からMPEG-4符号に変換する変換処理部223と、変換処理部223と接続し、MPEG-4符号に変換されたAVデータ（MPEG-4データ）を、再び暗号化する暗号化処理部224と、暗号化処理部224と接続し、暗号化されたAVデータをリアルタイムに、インターネットインターフェース（以下、単に「インターネットI/F」と呼ぶ）28を介して、インターネット16側に送信するリアルタイムトランスポートプロトコル(RTP)処理部225と、から構成される。

【0024】第1の認証・鍵交換部24は、インターネット16を介して、サーバー18内に蓄積された映像や音楽等のAVコンテンツの閲覧・参照等を要求する、各利用者の再生端末20に、識別ID（利用者ID）およびパスワード入力用ダイアログ画面を備えた利用者認証用ホームページおよびIEEE1394バス14に接続されたサーバー18や家電機器等を遠隔制御するため遠隔制御用ホームページを含む、各種のホームページを送信するホームページ処理部241と、利用者認証用ホームページのダイアログ画面から入力された利用者IDおよびパスワードが正規のものであるか否かを照合する利用者認証処理部242と、正規の利用者の再生端末20との間で認証・鍵交換処理を実行する第1の認証・鍵交換処理部243と、再生端末20とのやりとりをTCPパケット化するためのTCP処理部244と、から構成される。

【0025】第2の認証・鍵交換部26は、サーバー18との間で認証・鍵交換処理を実行する第2の認証・鍵交換処理部261と、サーバー18とのやりとりを非同期パケット化するための非同期データ処理部262と、から構成される。

【0026】次に、図3乃至図5を参照して、本発明の実施の形態に係る通信装置10の動作について説明する。図3は、本発明の実施の形態に係る通信装置10と、サーバー18および再生端末20と、の間の処理シーケンスチャートであり、図4および図5は、本発明の実施の形態に係る通信方法の処理手順を示すフローチャートである。

【0027】（1）図3のステップS101において、まず、再生端末20が、インターネット16を介して、通信装置10に対して、サーバー18内のデータを閲覧・参照するための遠隔制御用ホームページを要求する（図4のステップS201）。この遠隔制御用ホームページには、IEEE1394バス14に接続された、サーバー18や各種の家電機器を遠隔制御するためのボタンが少なくとも表示される。このボタンは、たとえばグラフィカルユーザインターフェース（Graphical User Interface; GUI）で構成される。

【0028】（2）図3のステップS102において、再生端末20からの遠隔制御用ホームページ要求を受けた通信装置10は、再生端末20に利用者認証用ホーム

8

ページを送信し、利用者IDおよびパスワードを要求する（図4のステップS202）。通信装置10は、この利用者IDおよびパスワードを要求し、ホームページを要求する再生端末20に利用者が、正規の利用者であるか否かを判断する。すなわち、要求されたホームページは、サーバー18や家電機器等の遠隔制御を可能とするものであり、正規の利用者以外にこのホームページを与えてしまうと、不審な人物にサーバー18や家電機器の制御をされかねない。そこで、通信装置10は、遠隔制御用ホームページを要求する再生端末20に対して、利用者IDおよびパスワードの入力を要求し、その利用者があらかじめ登録された、怪しくない人物であるか否かを確認する。

【0029】（3）図3のステップS103において、利用者IDおよびパスワードの入力を要求された再生端末20の利用者は、たとえば再生端末20に設けられたダイヤルキーを用いて、利用者IDおよびパスワードを入力する。再生端末20に入力された利用者IDおよびパスワードは、インターネット16を経由して、通信装置10に送信される。

【0030】（4）図3のステップS104において、再生端末20から送信された利用者IDおよびパスワードを受け取った通信装置10は、たとえば正規の利用者の利用者IDおよびパスワードを格納するデータベースを有している。そして、通信装置は、受け取った利用者IDおよびパスワードがそのデータベースに登録されているか否かを照合する（図4のステップS203）。利用者IDおよびパスワードが登録されていなければ（図4のステップS203NO）、直ちに、再生端末20との回線を切断する（図5のステップS204）。

【0031】（5）利用者IDおよびパスワードが登録されていれば（図4のステップS203YES）、図3のステップS105において、通信装置10は遠隔制御用ホームページを、インターネット16を介して、再生端末20に送信する（図5のステップS205）。そして、再生端末20の利用者は、遠隔制御用ホームページに表示された、サーバー18の制御用ボタンを操作することで、たとえば図6に示すようなコンテンツ選択画面を取得する。図6に示すように、このコンテンツ選択画面32には、「ホームサーバーに録画されている番組は以下の通りです。」と表示されており、利用者は、この選択画面32から、サーバー18内のコンテンツの再生が可能となる。すなわち、この選択画面32には、各コンテンツに対応付けられた、複数のボタン34（「ドラマ」34a、「スポーツ」34b、「ニュース」34c、「プライベートビデオ1」34d、「プライベートビデオ2」34e）が表示されており、各ボタン34を操作することで、各ボタン34に対応付けられたコンテンツを再生させることができる。なお、遠隔制御用ホームページを取得した利用者は、その遠隔制御用ホーム

ージの取得という事実によって、以降の手続きにおいて、IEEE1394バス14が配設された家庭12の住人と見なすことができる。

【0032】(6)図3のステップS106において、再生端末20に利用者が、たとえば「ドラマ」の再生を要求した場合、つまりボタン34aを操作すると(図4のステップS206)、図3のステップS107において、そのコンテンツ要求を受けた通信装置10は、サーバ18に、IEEE1394バス14を介して、たとえばオーディオ・ビジュアル・コントロール(AV/C)コマンドを用いて、コンテンツ送信要求のコマンドを発行する(図4のステップS207)。

【0033】(7)図3のステップS108において、コンテンツ「ドラマ」の送信要求を受けたサーバ18は、第1の暗号化鍵K1で暗号化されたコンテンツ「ドラマ」(MPEG-2データ)を、IEEE1394バス14を介して、通信装置10に送信する(図4のS207)。ここで、このコンテンツ「ドラマ」に書き込まれた暗号制御情報は、新たにこれ以上コピーを認めないという“No More Copy”であるとする。たとえば、IEEE1394における暗号化方式のデファクトスタンダードであるデジタルトランスミッションコンテンツプロテクション(DTCP)である。なお、暗号化されたAVデータ(コンテンツ「ドラマ」)は、IEEE1394バス上の同期チャンネルを通して送信される。

【0034】(8)図3のステップS109において、暗号化AVデータ(MPEG-2データ)を受信した通信装置10は、そのAVデータの暗号化の事実により、認証・鍵交換が必要であることを認識する。そして、通信装置10は、サーバ18との間で、認証・鍵交換処理を実行する(図4のステップS209)。この認証・鍵交換処理によって、通信装置10は、暗号化AVデータの復号のために必要な第1の復号鍵を入手する。たとえば、利用される暗号技術が共通鍵暗号であれば、第1の復号鍵は第1の暗号化鍵K1と同一である。

【0035】(9)図3のステップS110において、第1の復号鍵K1を入手した通信装置10は、先に受信したAVデータを復号する(図4のステップS210)。

【0036】(10)図3のステップS111において、抽出されたMPEG-2データであるAVデータを、MPEG-4データに変換して再圧縮する(図5のステップS211)。ここではMPEG-2/MPEG-4変換を実行しているが、他の例として、たとえばMPEG-2データの符号化速度を、インターネット16の通信帯域に適合するように、“絞る”、という形式を採っても良い。

【0037】(11)図3のステップS112において、通信装置10は、MPEG-4符号に変換されたAVデータを、第2の暗号化鍵K2を用いて再び暗号化する(図5のステップS212)。ここで、このAVデータは、元々暗号制御情報“No More Copy”が書き込まれたコンテンツ

である。すなわち、録画やコピーが禁止されたデータは、再送出の際にも、やはり録画やコピーを未然に防ぐ形式で送信されるべきである。したがって、変化された後でも、このAVデータには“No More Copy”が書き込まれることになる。また、この再暗号化が、図3のステップS102～S105の後に実行されるのは、最初にパスワード入力等によって、再生端末20の利用者が正規の利用者であると十分に予想され、このため、以降の手順が、利用者が個人的に楽しむための手順であることが明らかとなるからである。

【0038】(12)図3のステップS113において、通信装置10は、再暗号化されたAVデータ(MPEG-4データ)を、インターネット16を介して、再生端末20に送信する(図5のステップS213)。転送プロトコルとしてはRTPが利用される。また、再暗号化されたAVデータには、上述したように、暗号制御情報“No More Copy”が書き込まれる。したがって、再生端末20は、受け取ったAVデータを不正に蓄積することは不可能となる。

【0039】(13)図3のステップS114において、再暗号化AVデータ(MPEG-4データ)を受信した再生端末20は、そのAVデータの暗号化の事実により、認証・鍵交換が必要であることを認識する。そして、再生端末20は、通信装置10との間で、認証・鍵交換処理を実行する。この認証・鍵交換処理によって、再生端末20は、再暗号化AVデータの復号のために必要な第2の復号鍵を入手する。たとえば、利用される暗号技術が共通鍵暗号であれば、第2の復号鍵は第2の暗号化鍵K2と同一である。この再生端末20と通信装置10とのやりとりは、たとえばTCPパケットの形で行われる。

【0040】ここで、通信装置10は、再生端末20から認証・鍵交換処理要求を受けた場合(図5のステップS215)、その再生端末20の利用者が、図3のステップS102～S105の利用者認証によって、正規の利用者であると判断された者であるか否かを調べるのが望ましい(図5のステップS215)。正規の利用者でない場合、インターネット16を介して、不特定多数にコンテンツを送信してしまふことになりかねず、著作権法で定められた「個人で楽しむ限りにおいては、タイムシフトや加工等が許される」という原則に反するからである。図5のステップS215は、このようなことを未然に防止することが可能となる。もちろん、正規の利用者でなければ(図5のステップS215NO)、通信装置10は、直ちに、再生端末20との回線を切断する(図5のステップS204)。

【0041】このようにして、正規の利用者の再生端末20は、第2の復号鍵K2を他人に知られること無く取得することができ、受信された再暗号化AVデータを復号できる。ただし、上述したように、AVデータには“No More Copy”が書き込まれているので、再生端末20は、そ

11

のAVデータを蓄積／コピーすることはできない。その場で、デコード／表示させることができるだけである。

【0042】このように、本発明の実施の形態によれば、家庭網上で入手された、チャンネル作物を含む、あるいは著作物自体のAVデータを、公衆網に送信する場合に、その著作物の著作権法による保護を確実に実現することができる。

【0043】特に、近年のデジタル化・ネットワーク化の進展により、ネットワーク上で著作物を送信するという著作物の利用方法が発達・普及する現状にあつては、¹⁰ 本発明の重要性はきわめて高いものである。

【0044】

【発明の効果】本発明によれば、家庭網から公衆網へ著作物を送信する際に、その著作物の保護を確実に実行する通信装置を実現できる。

【0045】本発明によれば、家庭網から公衆網へ著作物を送信する際に、その著作物の保護を確実に実行する通信方法を実現できる。

【図面の簡単な説明】

【図1】本発明の実施の形態に係る通信装置によって接続された、家庭網と公衆網とからなるネットワーク・システムの全体構成を示すブロック図である。²⁰

【図2】本発明の実施の形態に係る通信装置の具体的な構成を示すブロック図である。

【図3】本発明の実施の形態に係る通信装置、サーバーおよび再生端末間で、著作物を含むAVデータを送受信する際の、処理シーケンスチャートである。

【図4】本発明の実施の形態に係る通信装置の通信方法の処理手順を示すフローチャートである（その1）。

【図5】本発明の実施の形態に係る通信装置の通信方法 *³⁰

12

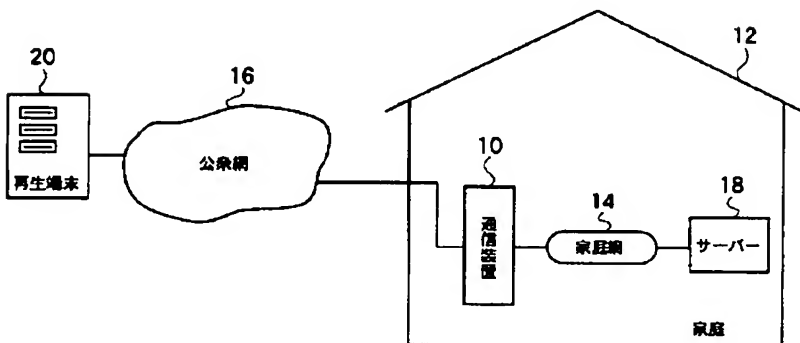
*の処理手順を示すフローチャートである（その2）。

【図6】本発明の実施の形態に係る通信装置から、再生端末に送信される、コンテンツ選択画面の内容を示す図である。

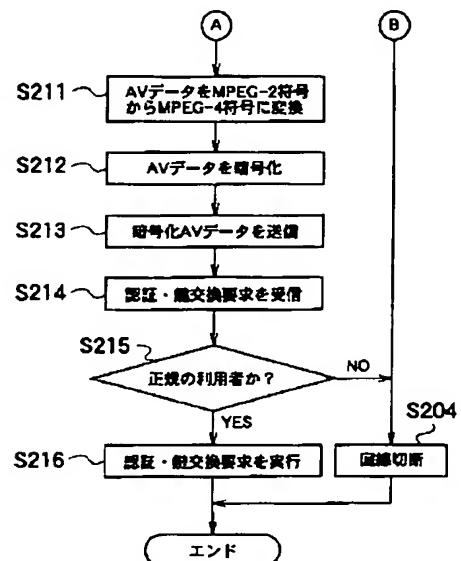
【符号の説明】

- 10 通信装置
- 12 家庭
- 14 家庭網
- 16 公衆網
- 18 サーバー
- 20 再生端末
- 22 送信部
- 24 第1の認証・鍵交換部
- 26 第2の認証・鍵交換部
- 28 インターネットインターフェース
- 30 IEEE1394インターフェース
- 32 コンテンツ選択画面
- 34 ボタン
- 221 同期データ処理部
- 222 復号処理部
- 223 変換処理部
- 224 暗号化処理部
- 225 RTP処理部
- 241 ホームページ処理部
- 242 利用者認証処理部
- 243 第1の認証・鍵交換処理部
- 244 TCP処理部
- 261 第2の認証・鍵交換処理部
- 262 非同期データ処理部

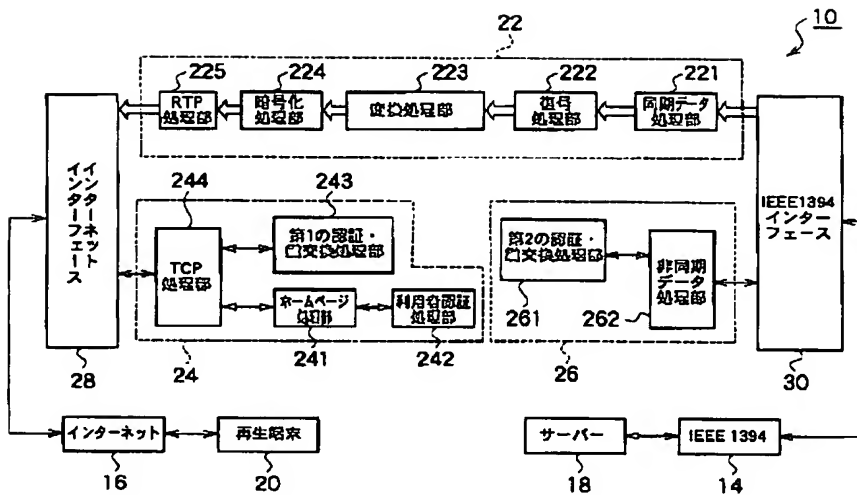
【図1】



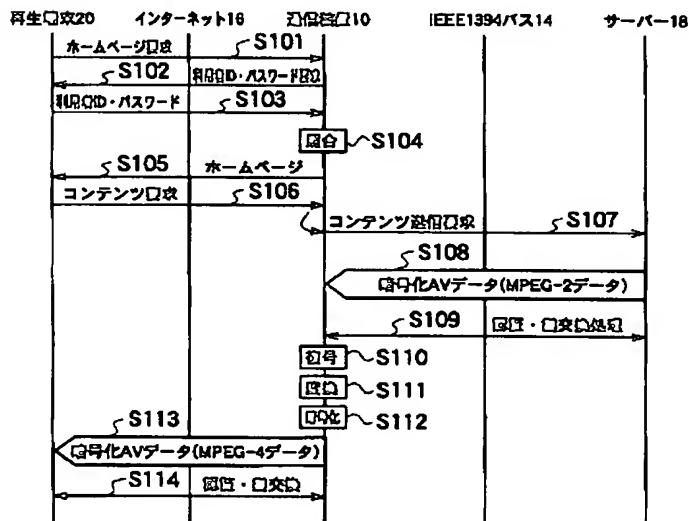
【図5】



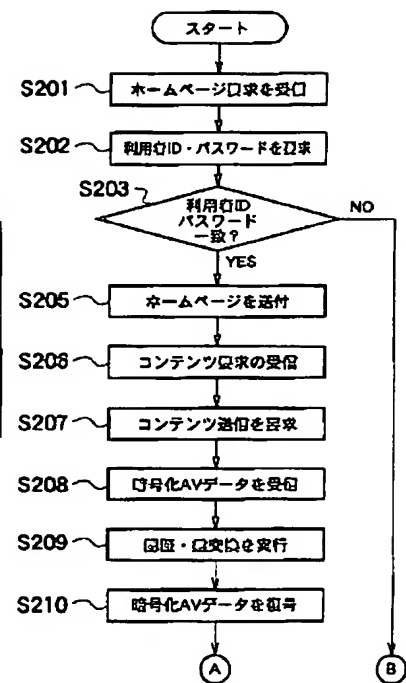
【図2】



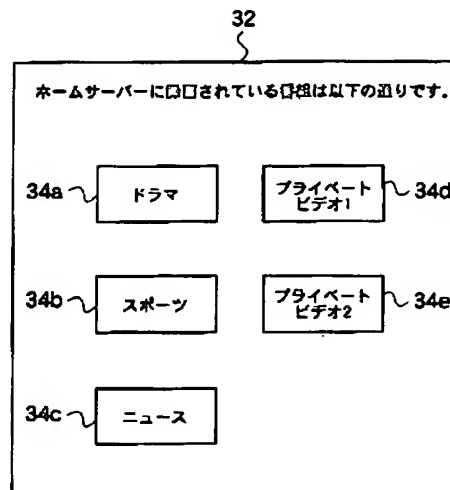
【図3】



【図4】



【図6】



フロントページの続き

Fターム(参考) 5J104 AA07 AA13 BA02 EA04 EA15
KA01 NA02 NA05
5K030 GA15 HB01 HB02 HC01 HC14
HD01 HD06
5K033 AA08 BA01 BA11 CB08 DA06
DA11 DA13 DB10 DB18
9A001 BB04 CC07 CC08 EE03 EE04
JJ25 JJ27 KK56 LL03